

ANALISIS *MALICIOUS TRAFFIC* PADA PONSEL ANDROID “*CHINA BRAND*” MENGGUNAKAN MALTRAIL

Tugas Akhir

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S-1
Program Studi Teknologi Informasi



Disusun oleh
PASKALIS RIVALDIANUS TAGANG
202104021

**FAKULTAS TEKNIK & TEKNOLOGI INFORMASI
UNIVERSITAS JENDERAL ACHMAD YANI
YOGYAKARTA
JUNI 2024**

HALAMAN PENGESAHAN

Tugas Akhir
ANALISIS MALICIOUS TRAFFIC PADA PONSEL ANDROID "CHINA
BRAND" MENGGUNAKAN MALTRAIL

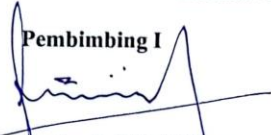
dipersiapkan dan disusun oleh

PASKALIS RIVALDIANUS TAGANG
202104021

telah dipertahankan di hadapan dewan penguji
pada tanggal 08 Juli 2024

Susunan Dewan Penguji

Pembimbing I


Ir. Dedy Hariyadi, S.T., M.Kom.
NIDN: 0518108001

Pembimbing II


Arief Ikhsan Wicaksono, S.Kom.,
M.Cs
NIDN: 0512128401

Penguji I


Rama Sahtyawan, S.T., M.Cs.
NIDN: 0518058001

Penguji II


Chanief Budi Setiawan, S.T., M.Eng
NIDN: 0514068101

Tugas akhir ini telah diterima sebagai
salah satu persyaratan untuk memperoleh gelar Sarjana
pada tanggal 11 Juli 2024

Ketua Program Studi S-1 Teknologi Informasi
Fakultas Teknik & Teknologi Informasi
Universitas Jenderal Achmad Yani Yogyakarta


Rama Sahtyawan, S.T., M.Cs.
NIDN: 0518058001



PERNYATAAN

Saya yang bertanda tangan di bawah ini, adalah mahasiswa Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta,

Nama : Paskalis Rivaldianus Tagang

NPM : 202104021

Program Studi : S-1 Teknologi Informasi

Judul Tugas Akhir : Analisis *Malicious Traffic* Pada Ponsel Android "*China Brand*" Menggunakan Maltrail

Saya menyatakan dengan sesungguhnya bahwa Tugas Akhir ini seluruhnya merupakan karya saya sendiri dan di dalamnya tidak memuat peniruan/plagiasi atas karya orang lain. Bagian-bagian tertentu dari karya tulis ini yang merupakan kutipan dari hasil karya orang lain telah dituliskan sumbernya secara jelas sesuai dengan norma, kaidah, dan etika penulisan karya ilmiah.

Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa dalam Tugas Akhir ini terkandung ciri-ciri plagiat dan bentuk-bentuk peniruan lain yang dianggap melanggar peraturan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Yogyakarta, 11 Juli 2024



Paskalis Rivaldianus Tagang

KATA PENGANTAR

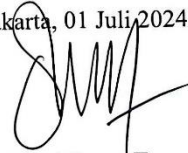
Puji syukur penulis panjatkan ke hadirat Allah SWT atas limpahan rahmat-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir yang berjudul: “Analisis *Malicious Traffic* Pada Ponsel Android “*China Brand*” Menggunakan Maltrail”. Penyusunan laporan ini merupakan salah satu persyaratan untuk menyelesaikan studi di Program Studi S-1 Sistem Informasi Fakultas Teknik & Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta. Laporan ini dapat diselesaikan atas bimbingan, arahan, dan bantuan dari berbagai pihak. Pada kesempatan ini penulis dengan rendah hati mengucapkan terima kasih dengan setulus-tulusnya kepada:

1. Bapak Aris Wahyu Murdiyanto, S.Kom., M.Cs. selaku Dekan Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
2. Bapak Rama Sahtyawan, S.T., M.Cs. selaku Ketua Program Studi S-1 Teknologi Informasi Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
3. Bapak Ir. Dedy Hariyadi, S.T., M.Kom. dan Bapak Arief Ikhwan Wicaksono, S.Kom., M.Cs selaku Dosen Pembimbing Tugas Akhir
4. Para dosen yang telah memberikan banyak bekal ilmu pengetahuan kepada penulis selama menjadi mahasiswa di Fakultas Teknik dan Teknologi Informasi Universitas Jenderal Achmad Yani Yogyakarta;
5. Keluarga tercinta, sahabat-sahabat saya, yang memberikan dukungan penulis dalam menempuh studi sarjana. Rekan-rekan mahasiswa Prodi S-1 Teknologi Informasi di Universitas Jenderal Achmad Yani Yogyakarta yang sudah memberi dukungan dan kerja sama selama pembuatan tugas akhir.

Penulis menyadari bahwa laporan tugas akhir ini masih jauh dari kata sempurna. Maka dari itu dengan segala kerendahan hati penulis sangat menghargai

adanya kritik dan saran yang membangun dari semua pihak yang bersedia meluangkan waktu untuk membaca laporan tugas akhir ini.

Yogyakarta, 01 Juli 2024



Paskalis Rivaldianus Tagang

PERPUSTAKAAN
JENDERAL ACHMAD YANI
YOGYAKARTA
UNIVERSITAS

DAFTAR ISI

Judul.....	i
Halaman Pengesahan.....	ii
Pernyataan	iii
Kata Pengantar	iv
Daftar Isi	vi
Daftar Tabel.....	viii
Daftar Gambar	ix
Daftar Lampiran	x
Daftar Singkatan	xi
Intisari.....	xii
Abstract.....	xiii
Bab 1 Pendahuluan	1
1.1 Latar Belakang	1
1.1.1 Perumusan Masalah.....	3
1.1.2 Manfaat Hasil Penelitian	3
1.1.3 Pertanyaan Penelitian	4
1.2 Tujuan Penelitian	4
Bab 2 Tinjauan Pustaka dan Landasan Teori.....	5
2.1 Tinjauan Pustaka	5
2.2 Landasan Teori.....	13
2.2.1 Jaringan Nirkabel	13
2.2.2 <i>Port Mirroring</i>	14
2.2.3 <i>IDS (Intrusive Detection System)</i>	14
2.2.4 <i>Malicious Traffic</i>	14
2.2.5 <i>Maltrail</i>	15
Bab 3 Metode Penelitian.....	16
3.1 Bahan dan alat Penelitian	17
3.1.1 Ponsel Android	17

3.1.2	Raspberry Pi 4	17
3.1.3	MikroTik	18
3.1.4	Access Point	18
3.2	Jalan Penelitian.....	18
Bab 4	Hasil Penelitian.....	20
4.1	Ringkasan Hasil Penelitian	20
4.1.1	Proses Pengumpulan Data.....	20
4.1.1.1	<i>Port Mirroring</i>	20
4.1.1.2	<i>IDS (Intrusion Detection System)</i>	21
4.1.1.3	Instalasi Raspberry.....	22
4.1.1.4	Setup MikroTik Dasar.....	30
4.1.2	Pelaporan hasil analisis	32
Bab 5	Kesimpulan dan Saran	38
5.1	Kesimpulan	38
5.2	Saran.....	38
	Daftar Pustaka.....	39
	Lampiran	42

DAFTAR TABEL

Table 1 <i>Literature Review</i>	6
Table 2 Hasil jumlah trafik pada ponsel Android	37

PERPUSTAKAAN
JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR GAMBAR

Gambar 3.1 <i>Port Mirroring</i>	16
Gambar 3.2 Alur Penelitian	19
Gambar 4.1 Metode <i>Port Mirroring</i>	21
Gambar 4.2. Tampilan imager Raspberry Pi	22
Gambar 4.3 konfigurasi SSH.....	23
Gambar 4.4 SSH diaktifkan.....	24
Gambar 4.5 menu antarmuka nmtui	25
Gambar 4.6 menu antarmuka jaringan	25
Gambar 4.7 menu antarmuka jaringan	25
Gambar 4.8 mengatur konfigurasi IPv4	26
Gambar 4.9 mengatur konfigurasi IPv4	26
Gambar 4.10 Tampilan setelah pemilihan.....	27
Gambar 4.11 mengatur konfigurasi IPv4	27
Gambar 4.12 Mengatur IP Address, Gateway, dan DNS server	28
Gambar 4.13 tampilan antarmuka nmtui	28
Gambar 4.14 Pengaturan antarmuka jaringan	29
Gambar 4.15 Pengaturan antarmuka jaringan	29
Gambar 4.16 Topologi Jaringan	31
Gambar 4.17 Tampilan WinBox	32
Gambar 4.18 Instalasi Maltrail	34
Gambar 4.19 Hasil <i>Malicious traffic</i> ponsel android X1.....	35
Gambar 4.20 Hasil <i>Malicious traffic</i> ponsel android X2.....	35
Gambar 4.21 Hasil <i>Malicious traffic</i> ponsel android X3.....	36
Gambar 4.22 Hasil <i>Malicious traffic</i> ponsel android X4.....	36
Gambar 4.23 Hasil <i>Malicious traffic</i> ponsel android X5.....	36

DAFTAR LAMPIRAN

Lampiran 1 Surat Ijin Penelitian	42
Lampiran 2 Dokumentasi pemasangan alat dan pemantuan	43
Lampiran 3 Proses Penelitian	44
Lampiran 4 Lembar Bimbingan Dosen	45
Lampiran 5 Hasil Cek Plagirisme	45

PERPUSTAKAAN
JENDERAL ACHMAD YANI
YOGYAKARTA

DAFTAR SINGKATAN

APT	<i>Advanced Persistent Threat</i>
NDLC	<i>Network Development Life Cycle</i>
ML	<i>Machine Learning</i>
GAB	<i>Global Attention Block</i>
CAB	<i>Category Attention Block</i>
DDoS	<i>Distributed Denial of Service</i>
SVM	<i>Support Vector Machine</i>
RF	<i>Random Forest</i>
HexCNN-1D	<i>Convolutional Neural Network</i>
WLAN	<i>Wireless Local Area Network</i>
IDS	<i>Intrusive Detection System</i>
NIDS	<i>Network Intrusive Detection System</i>
TAP	<i>Test Acces Point</i>
OS	<i>Operating System</i>
DHCP	<i>Dynamic Host Configuration Protocol</i>